PATENT
PD-200290

DISTRIBUTION OF VIDEO CONTENT USING A TRUSTED NETWORK KEY FOR SHARING CONTENT

Inventors:

Raynold M. Kahn
Gregory J. Gagnon
Christopher P. Curren
Thomas H. James

DISTRIBUTION OF VIDEO CONTENT USING A TRUSTED NETWORK KEY FOR SHARING CONTENT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to the following co-pending and commonly-assigned patent applications, all of which applications are incorporated by reference herein:

U.S. Patent Application Serial No. 09/620,832, entitled "VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200055, filed on July 21, 2000;

U.S. Patent Application Serial No. 09/620,833, entitled "SECURE STORAGE AND REPLAY OF MEDIA PROGRAMS USING A HARD-PAIRED RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200042, filed on July 21, 2000;

U.S. Patent Application Serial No. 09/621,476, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN A HARD-PAIRED RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200043, filed on July 21, 2000;

U.S. Patent Application Serial No. 09/620,773, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH MODIFIED CONDITIONAL ACCESS FUNCTIONALITY, " by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-20044, filed on July 21, 2000;

U.S. Patent Application Serial No. 09/620,772, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH SMARTCARD GENERATED KEYS," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200045, filed on July 21, 2000;

U.S. Patent Application Serial No. 09/491,959, entitled "VIRTUAL VIDEO ON DEMAND USING MULTIPLE ENCRYPTED VIDEO SEGMENTS," by Robert G. Arsenault and Leon J. Stanger, attorney's docket number PD-980208, filed on January 26, 2000;

Application Serial No. 09/960,824, entitled "METHOD AND APPARATUS FOR ENCRYPTING MEDIA PROGRAMS FOR LATER PURCHASE AND VIEWING," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, Ronald P. Cocchi, and Thomas H. James, attorney's docket number PD-200176, filed September 21, 2001;

Application Serial No. 09/954,236, entitled "EMBEDDED BLACKLISTING FOR DIGITAL BROADCAST SYSTEM SECURITY," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, and Dennis R. Flaherty, attorney's docket number PD-200125, filed September 14, 2001;

U.S. Patent Application Serial No. --/---,---, entitled "METHOD AND APPARATUS FOR ENSURING RECEPTION OF CONDITIONAL ACCESS INFORMATION IN MULTI-TUNER RECEIVERS," by Peter M. Klauss, Raynold M. Kahn, Gregory J. Gagnon, and David D. Ha, attorney's docket number PD-200183, filed on November 21, 2002;

U.S. Patent Application Serial No. --/---,---, entitled "METHOD AND APPARATUS FOR MINIMIZING CONDITIONAL ACCESS INFORMATION OVERHEAD WHILE ENSURING CONDITIONAL ACCESS INFORMATION RECEPTION IN MULTI-TUNER RECEIVERS," by Peter M. Klauss, Raynold M. Kahn, Gregory J. Gagnon, and David D. Ha, attorney's docket number PD-200184, filed on November 21, 2002;

PCT international Patent Application Serial No. US02/29881, entitled "METHOD AND APPARATUS FOR CONTROLLING PAIRED OPERATION OF A CONDITIONAL ACCESS MODULE AND AN INTEGRATED RECEIVER AND DECODER," by Raynold M. Kahn and Jordan Levy, attorney's docket number PD-200176A PCT, filed on September 20, 2002;

U.S. Patent Application Serial No. --/---,---, entitled "DISTRIBUTION OF VIDEO CONTENT USING CLIENT TO HOST PAIRING OF INTEGRATED

RECEIVERS/DECODERS," by Raynold M. Kahn, Greg Gagnon, Christopher P. Curren and Thomas H. James, attorney's docket number PD-200289, filed on same date herewith; and

U.S. Patent Application Serial No. --/---,---, entitled "DISTRIBUTION OF BROADCAST CONTENT FOR REMOTE DECRYPTION AND VIEWING," by Raynold M. Kahn, Ronald Cocchi and Gregory J. Gagnon, attorney's docket number PD-200292, filed on same date herewith.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for distributing video content using a trusted network key for sharing content.

2. Description of the Related Art

Direct broadcast satellite (DBS) systems have become commonplace in recent years. DBS systems have been designed to assure that only paying subscribers receive program materials transmitted by service providers. Among such systems are those which use a conditional access module (typically in the form of a smartcard) that can be removably inserted into the receiver.

One of the current disadvantages of existing DBS receivers is that every television requires a separate integrated receiver/decoder (IRD) in order to receive unique programming. Moreover, each IRD requires a tuner and conditional access module in order to receive and decrypt the programming. In addition, each of the IRDs require a separate disk drive in order to provide digital video record (DVR) capabilities. All of these components drive up the cost of the IRDs.

Currently, there is no method of securely sharing content between connected IRDs, such as a host IRD connected to authorized client IRDs. One of the key reasons is that the prior art provides no method for the service provider to know of and selectively enable the authorized client IRDs. As a result, service providers have no method of preventing widespread, and possible unauthorized, distribution of their program materials if several IRDs are networked together.

The present invention describes a network architecture that includes a central or host IRD and one or more lightweight secondary or client IRDs coupled thereto. The present invention also describes a method of securely passing program materials between the host and client IRDs in the network and a method for the host IRD to know which other client IRDs are allowed on the network using a host-client relationship.

Since these client IRDs are known and trusted by the host IRD, the host IRD can transmit program materials to the client IRDs. This means that the client IRDs would not require a tuner, conditional access module, or disk drive, since the host IRD is responsible for the reception and storage of the program materials, and the conditional access module associated with the host IRD is responsible for the reception of media encryption keys for program decryption by host and client IRDs. This allows distribution of the program materials throughout a household or other location at a significantly reduced cost as compared to other schemes, which require full IRDs for each individual subscriber.

SUMMARY OF THE INVENTION

In summary, the present invention describes a method, apparatus and article of manufacture for distributing video content from a direct broadcast satellite system between a host receiver and a client receiver.

A family pairing key is transmitted from the direct broadcast satellite system to both the host receiver and the client receiver. The family pairing key is decrypted at the host receiver using a receiver key uniquely associated with the host receiver, and the family pairing key is decrypted at the client receiver using a receiver key uniquely associated with the client receiver.

Program materials are received by the host receiver from the direct broadcast satellite system. The program materials received by the host receiver are encrypted using a media encryption key and the host receiver uses the media encryption key to decrypt the program materials .

The decrypted program materials are then encrypted at the host receiver using a copy protection key. The copy protection key is generated by the host receiver using content information decrypted by the family pairing key. The content information may comprise a content identifier obtained from the program materials.

The encrypted program materials are transferred from the host receiver to the client receiver.

The encrypted program materials are then decrypted at the client receiver using the copy protection key. Like the host receiver, the copy protection key is generated by the client receiver using content information decrypted by the family pairing key. The content information may comprise a content identifier obtained from the program materials.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram illustrating an overview of a direct broadcast satellite system according to a preferred embodiment of the present invention;

FIG. 2 is a block diagram showing a typical uplink configuration for a single satellite transponder, showing how program materials and program control information are uplinked to the satellite by the control center and the uplink center;

FIG. 3A is a diagram of a representative data stream according to the preferred embodiment of the present invention;

FIG. 3B is a diagram of a representative data packet according to the preferred embodiment of the present invention;

FIG. 4 is a simplified block diagram of an integrated receiver/decoder according to the preferred embodiment of the present invention;

FIG. 5 is a logical flow illustrating how the host IRD and CAM are operatively paired according to the preferred embodiment of the present invention;

FIG. 6 is a logical flow illustrating how the host and client IRDs are operatively paired according to the preferred embodiment of the present invention; and

FIG. 7 is a logical flow illustrating how the program materials may be shared between host and client IRDs according to the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which show, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

DIRECT BROADCAST SATELLITE SYSTEM

FIG. 1 is a diagram illustrating an overview of a direct broadcast satellite system 100 according to a preferred embodiment of the present invention. The system 100 includes a control center 102 operated by a service provider in communication with an uplink center 104 via a ground link 106 and with subscriber receiving stations 108 via a link 110. The control center 102 provides program materials to the uplink center 104 and coordinates with the subscriber receiving stations 108 to offer various services, including key management for encryption and decryption, pay-per-view (PPV), billing, etc.

The uplink center 104 receives the program materials from the control center 102 and, using an uplink antenna 112 and transmitter 114, transmits the program materials to one or more satellites 116, each of which may include one or more transponders 118. The satellites 116 receive and process this program material, and re-transmit the program materials to subscriber receiving stations 108 via downlink 120 using transmitter 118. Subscriber receiving stations 108 receive the program materials from the satellites 116 via an antenna 122, and decrypt and decode the program materials using an integrated receiver/decoder (IRD) 124.

UPLINK CONFIGURATION

FIG. 2 is a block diagram showing a typical uplink center 104 configuration for a single transponder 118, showing how program materials and program control information are uplinked to the satellite 116 by the control center 102 and the uplink center 104.

One or more channels are provided by program sources 200A-200C, which may comprise one or more video channels augmented respectively with one or more audio channels.

The data from each program source 200A-200C is provided to a corresponding encoder 202A-202C, which in one embodiment comprise Motion Picture Experts Group (MPEG) encoders, although other encoders can be used as well. After encoding by the encoders 202A-202C, the output therefrom is converted into data packets by corresponding packetizers 204A-204C.

In addition to the program sources 200A-200C, data source 206 and conditional access manager 208 may provide one or more data streams for transmission by the system 100. The data from the data source 206 and conditional access manager 208 is provided to a corresponding encoder 202D-202E. After encoding by the encoders 202D-202E, the output therefrom is converted into data packets by corresponding packetizers 204D-204E.

A system channel identifier (SCID) generator 210, null packet (NP) generator 212 and system clock 214 provide control information for use in constructing a data stream for transmission by the system 100. Specifically, the packetizers 204A-204F assemble data packets using a system clock reference (SCR) from the system clock 214, a control word (CW) generated by the conditional access manager 208, and a system channel identifier (SCID) from the SCID generator 210 that associates each of the data packets that are broadcast to the subscriber with a program channel.

Each of the encoders 202A-202C also accepts a presentation time stamp (PTS) from a multiplex controller 216. The PTS is a wrap-around binary time stamp that is used to assure that the video channels are properly synchronized with the audio channels after encoding and decoding.

Finally, these data packets are then multiplexed into a serial data stream by the controller 216. The data stream is then encrypted by an encryption module 218, modulated by a modulator 220, and provided to a transmitter 222, which broadcasts the modulated data stream on a frequency bandwidth to the satellite 116 via the antenna 106.

REPRESENTATIVE DATA STREAM

FIG. 3A is a diagram of a representative data stream 300 according to the preferred embodiment of the present invention. The first packet 302 comprises information from video channel 1 (data coming from, for example, the first program source 200A); the second packet 304 comprises computer data information (that was

obtained, for example, from the computer data source 206); the third packet 306 comprises information from video channel 3 (from one of the third program source 200C); the fourth packet 308 includes information from video channel 1 (from the first program source 200A); the fifth packet 310 includes a null packet (from the NP generator 212); the sixth packet 312 includes information from audio channel 1 (from the first program source 200A); the seventh packet 314 includes information from video channel 1 (from the first program source 200A); and the eighth packet 316 includes information from video channel 2 (from the second program source 200B). The data stream therefore comprises a series of packets from any one of the program and/or data sources in an order determined by the controller 216. Using the SCID, the IRD 124 reassembles the packets to regenerate the program materials for each of the channels.

FIG. 3B is a diagram of a representative data packet 318 according to the preferred embodiment of the present invention. Each data packet segment 318 is 147 bytes long, and comprises a number of packet segments 320-326. The first segment 320 comprises two bytes of information containing the SCID and flags. The SCID is a unique 12-bit number that uniquely identifies the channel associated with the data packet 318. The flags include 4 bits that are used to control whether the data packet 318 is encrypted, and what key must be used to decrypt the data packet 318. The second segment 322 is made up of a 4-bit packet type indicator and a 4 -bit continuity counter. The packet type identifies the packet as one of the four data types (video, audio, data, or null). When combined with the SCID, the packet type determines how the data packet 318 will be used. The continuity counter increments once for each packet type and SCID. The third segment 324 comprises 127 bytes of payload data. The fourth segment 326 is data required to perform forward error correction on the data packet 318.

ENCRYPTION OF PROGRAM MATERIALS

As noted above, program materials are encrypted by the encryption module 218 before transmission to ensure that they are received and viewed only by authorized IRDs 124. The program materials are encrypted according to an encryption key referred to hereinafter as a control word (CW). This can be accomplished by a variety of data encryption techniques, including symmetric algorithms, such as the data encryption

standard (DES), and asymmetric algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm.

To decrypt the program material, the IRD 124 must also have access to the associated CW. To maintain security, the CW is not transmitted to the IRD 124 in plaintext. Instead, the CW is encrypted before transmission to the IRD 124. The encrypted CW is transmitted to the IRD 124 in a control word packet (CWP), i.e., a data packet type as described in FIG. 3B.

In one embodiment, the data in the CWP, including the CW, is encrypted and decrypted via what is referred to hereinafter as an input/output (I/O) indecipherable algorithm. An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that its characteristics cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are non-stationary (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at another time.

So long as the encryption module 218 and the IRD 124 share the same I/O indecipherable algorithm, the IRD 124 can decode the information in the encrypted CWP to retrieve the CW. Then, using the CW, the IRD 124 can decrypt the program materials so that it can be displayed or otherwise presented.

INTEGRATED RECEIVER/DECODER

FIG. 4 is a simplified block diagram of an IRD 124 according to the preferred embodiment of the present invention. The IRD 124 includes a tuner 400, a transport and demultiplexing module (TDM) 402 that operates under the control of a microcontroller 404 to perform transport, demultiplexing, decryption and encryption functions, a source decoder 406, random access memory (RAM) 408, external interfaces 410, user I/O 412, a conditional access module (CAM) 414, and conditional access verifier (CAV) 416.

The tuner 400 receives the data packets from the antenna 122 and provides the packets to the TDM 402. Using the SCIDs associated with the program materials, the TDM 402 and microcontroller 404 reassemble the data packets according to the channel selected by the subscriber and indicated by the user I/O 412, and decrypt the program materials using the CW.

Once the program materials have been decrypted, they are provided to the source decoder 406, which decodes the program materials according to MPEG or other standards as appropriate. The decoded program materials may be stored in the RAM 408 or provided to devices coupled to the IRD 124 via the external interfaces 410, wherein the devices coupled to the IRD 124 can include or a media storage device 418, such as a disk drive, a presentation device 420, such as a monitor, or a networked device, such as another IRD 124.

The CAM 414 is typically implemented in a smartcard or similar device, which is provided to the subscriber to be inserted into the IRD 124. The CAM 414 interfaces with the CAV 416 and the TDM 402 to verify that the IRD 124 is entitled to access the program materials .

The CW is obtained from the CWP using the CAV 416 and the CAM 414. The TDM 402 provides the CWP to the CAM 414 via the CAV 416. The CAM 414 uses an I/O indecipherable algorithm to generate the CW, which is provided back to the TDM 402. The TDM 402 then uses the CW to decrypt the program materials .

In one embodiment including a plurality of networked IRDs 124, one of the IRDs 124 is designated a "host IRD" and each of the other IRDs are designated as a "client IRD". In such an embodiment, the host IRD 124 includes all of the components described in FIG. 4, while the client IRDs 124 are simpler and do not include a tuner 400, CAM 414, CAV 416, disk drive 418, or other components, in order to reduce the cost of the client IRD 124. The client IRD 124 can be used to request program materials that are received or reproduced by the host IRD 124, thus allowing program materials to be reproduced at other locations in the home.

However, in this embodiment, all of the IRDs 124 in a "family" share a family pairing key (FPK) that is generated by the service provider for the purposes of sharing the program materials among the IRDs 124 in the family. Consequently, the FPK is a trusted

network key for sharing content between a host IRD 124 and one or more client IRDs 124.

OPERATIVE PAIRING THE HOST IRD AND CAM

FIG. 5 is a logical flow illustrating how the host IRD 124 and CAM 414 are operatively paired according to the preferred embodiment of the present invention.

After the subscriber has purchased and installed the host IRD 124 and associated hardware, the subscriber supplies a unique identifier (such as a serial number) for the host IRD 124 to the service provider. The unique identifier is itself uniquely associated with a secret receiver key (RK). This association is implemented in the IRD 124 itself, and is known to the service provider. Thereafter, the service provider determines a pairing key (PK) that will be used to encrypt communications between the CAM 414 and the IRD 124.

The PK is then encrypted by the service provider using the RK, to produce an encrypted PK, denoted ER(PK), wherein the ER( ) indicates that RK encryption is used and the PK indicates that the PK is encrypted. A message for the CAM 414 comprising the PK and the ER(PK) is generated by the service provider, and the message is encrypted using a conditional access message encryption algorithm to produce EM(PK, ER(PK)), wherein the EM( ) indicates that conditional access message encryption is used and the PK, ER(PK) indicates that the PK, ER(PK) is encrypted.

The EM(PK, ER(PK)) is then transmitted to the IRD 124 where it is received by the tuner 400 and TDM 402. The TDM 402 routes data packets with the encrypted message EM(PK, ER(PK)) to the CAM 414 for decryption.

In the CAM 414, the EM(PK,ER(PK)) is decrypted by a message decryption algorithm (EM DECR) 500 to produce the decrypted PK, which is stored in a secure memory 502 in the CAM 414. The ER(PK) is provided from the CAM 414 to the TDM 402, and since it is encrypted using the RK, it is not exposed in plaintext. (In the preferred embodiment, the ER(PK) is delivered to the TDM 402 via the CAM 414, but alternative embodiments might deliver ER(PK) directly to the TDM 402).

In the TDM 402, the ER(PK) is decrypted by an Advanced Encryption Standard (AES) decryption algorithm (AES DECR) 504 using the RK 506 to produce the decrypted

PK, which is then stored in a secure memory 508. This PK, now stored in both the IRD 124 and the CAM 414, is used to encrypt communications between the CAM 414 and the IRD 124, as desired.

For example, using the PK, the CAM 414 encrypts the CW to produce EPK(CW), wherein the EPK( ) indicates that PK encryption is used and the CW indicates that the CW is encrypted. The TDM 402 decrypts the EPK(CW) received from the CAM 414. Since the EPK(CW) can only be decrypted by an IRD 124 that contains the appropriate PK, this cryptographically binds ("pairs") the CAM 414 and the IRD 124.

OPERATIVELY PAIRING THE HOST AND CLIENT IRDS

FIG. 6 is a logical flow illustrating how the host and client IRDs 124 are operatively paired according to the preferred embodiment of the present invention.

The present invention also provides for pairing between a host IRD 124 and one or more client IRDs 124, to ensure that program materials are never shared between the host IRD 124 and client IRDs 124 in plaintext. The pairing of the host IRD 124 and client IRDs 124 is accomplished by the use of a family pairing key (FPK).

As noted above, the subscriber supplies a unique identifier (such as a serial number) for the host IRD 124 to the service provider, wherein the unique identifier is associated with a secret receiver key (RK), wherein the association is implemented in the IRD 124 itself and is known to the service provider.

After activating the host IRD 124, the subscriber can request the activation of additional client IRDs 124 using the same method. Consequently, the service provider would determine the RK for each of the client IRDs 124 as well.

Thereafter, the service provider establishes the FPK for a particular combination of host and client IRDs 124. Preferably, the service provider encrypts the FPK, using the AES encryption algorithm, with RKH, the RK of the host IRD 124, and RKC, the RK of the client IRD 124, thereby creating two ER(FPK) messages containing the encrypted FPK, i.e., ERH(FPK) for the host IRD 124 and ERC(FPK) for the client IRD 124.

The service provider transmits one or more messages to the host IRD 124, as represented by 600, using an ID for the CAM 414 of the host IRD 124 for over-the-air addressing of the message, and specifying both a Host ID (HID) and a Client ID (CLID),

wherein the CLID identifies the client IRDs 124 to the host IRD 124. These messages contain the encrypted FPK, and are then stored on disk drive 418 or other non-volatile memory in the host IRD 124.

Any number of such encrypted versions of the FPK can be stored in the host IRD 124. For example, there may be a different FPK for each pairing of a client IRD 124 networked with the host IRD 124. On the other hand, a host IRD 124 may share the same FPK with all the client IRDs 124.

Preferably, the host IRD 124 receives both of the ERH(FPK) and ERC(FPK) messages off-air and, at some later time, the ERC(FPK) for the client IRD 124 is obtained by the client IRD 124 from the host IRD 124. This may occur, for example, when a client IRD 124 is activated or powered up.

In the host and client IRDs 124, the ER(FPK) (which is either the ERH(FPK) or ERC(FPK)) is decrypted by an AES decryption algorithm (AES DECR) 602 in the TDM 402 using the appropriate RK 604 (which is either the RKH or RLC), and the decrypted FPK is stored in a secure memory 606 in the host and client IRDs 124.

Consequently, the service provider, through the assignment of the FPK, establishes a family pairing relationship between the host IRD 124 and one or more client IRDs 124 forming a network, so that the program materials are shared in secure manner within the network.

SHARING PROGRAM MATERIALS BETWEEN HOST AND CLIENT IRDS

FIG. 7 is a logical flow illustrating how the program materials may be shared between host and client IRDs 124 according to the preferred embodiment of the present invention.

In the portion of FIG. 7 labeled "Off-Air Receive," the host IRD 124 receives a data stream including the program materials encrypted by the media encryption key CW, as well as the encrypted media encryption key EI(CW) itself. The EI(CW) is provided, via the TDM 402, to the CAM 414, where it is decrypted by an I/O indecipherable algorithm (EI DECR) 700. The result is the unencrypted media encryption key CW.

The unencrypted CW is then re-encrypted by the CAM 414 by an AES encryption algorithm (AES ENCR) 702 using the PK 704 stored in the CAM 414 to produce a re-encrypted media encryption key EPK(CW).

The re-encrypted media encryption key EPK(CW) is provided to the TDM 402, where it is decrypted by an AES decryption algorithm (AES DECR) 706 using the PK 708 stored in the TDM 402, in order to obtain the unencrypted media encryption key (CW). The unencrypted CW is then stored in a CW storage 710, and used when necessary by a Data Encryption Standard (DES) decryption algorithm (DES DECR) 712 to decrypt the program material.

In the portion of FIG. 7 labeled "Transmit to Client IRD," content identification (CID) information 714 is decrypted by an AES decryption algorithm (AES DECR) 716 using the FPK 718 stored in the TDM 402, in order to generate a CP session key for encrypting and decrypting the program materials shared with the client IRD 124. The CID information 714 preferably comprises a content identifier, and is obtained from properties and/or metadata of the program materials .

After the CP session key is generated by the AES decryption algorithm 716, the CP session key is then stored in the memory 720 of the TDM 402. Thereafter, the CP session key is retrieved from the memory 720 of the TDM 402 for use in encrypting the program materials by an AES encryption algorithm (AES ENCR) 722.

Thereafter, the encrypted program materials are transferred from the host receiver 124 to the client receiver 124, as represented by 724.

Since the program materials are encrypted with the CP session key generated by the host IRD 124, the client IRD 124 must be able to generate the same CP session key as the host IRD 124. This task is accomplished in same manner as the host IRD 124.

In the portion of FIG. 7 labeled "Read from Host IRD and Display," content identification (CID) information 726 is decrypted by an AES decryption algorithm (AES DECR) 728 using the FPK 732 stored in the TDM 402, in order to generate a CP session key for encrypting and decrypting the program materials shared by the host IRD 124. As above, the CID information 726 preferably is derived from properties and/or metadata of the program materials .

After the CP session key is generated by the AES decryption algorithm 728, the CP session key is then stored in the memory 732 of the TDM 402. Thereafter, the CP session key is retrieved from the memory 732 of the TDM 402 for use in decrypting the program materials by an AES decryption algorithm (AES ENCR) 734. The client IRD 124 can then display the program materials on a presentation device 420 coupled to the client IRD 124.

Because this method does not require the client IRD 124 to perform any traditional conditional access tasks, no CAM 414 is required in the client IRD 124. Also, since the client IRD 124 does not need to receive the program materials from an off-air signal, no tuner 400 is required. Finally, no disk drive 418 is required for the client IRD 124, since the client IRD 124 may use the disk drive 418 of the host IRD 124 as a "virtual disk." All of this greatly reduces the cost of the client IRDs 124, which in turn reduces the cost of distributing the program materials throughout a house or other building, while maintaining the security of the program materials.

Since this technique allows one key to be used by all members of a family of IRDs 124, it allows every IRD 124 in the family to be able to share the program materials equally. This greatly simplifies key distribution, but the service provider loses some control over where the program materials are transmitted. This issue can be overcome by careful system planning and would not be considered a significant roadblock.

CONCLUSION

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching.

For example, while the foregoing disclosure presents an embodiment of the present invention as it is applied to a direct broadcast satellite system, the present invention can be applied to any system that uses encryption. Moreover, although the present invention is described in terms of specific encryption and decryption schemes, it could also be applied to other encryption and decryption schemes, or to different uses of the specific encryption and decryption schemes. Finally, although specific hardware,

software and logic is described herein, those skilled in the art will recognize that other hardware, software or logic may accomplish the same result, without departing from the scope of the present invention.

It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.